UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/686,694	10/15/2003	Joshua Haghpassand	4839/4	9174

44696 7590 12/02/2011

DR. MARK M. FRIEDMAN
Moshe Aviv Tower, 54th Floor, 7 Jabotinsky St.
Ramat Gan, 52520
ISRAEL

EXAMINER	
SWEARINGEN, JEFFREY R	

ART UNIT	PAPER NUMBER
2445	

NOTIFICATION DATE	DELIVERY MODE
12/02/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@friedpat.com
friedpat.uspto@gmail.com
nomi_m@friedpat.com

Office Action Summary	Application No.	Applicant(s)	
	10/686,694	HAGHPASSAND, JOSHUA	
	Examiner	Art Unit	
	Jeffrey R. Swearingen	2445	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 September 2011*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-3,6,9-14,17-21 and 23-57* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-3,6,9-14,17-21 and 23-57* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Terminal Disclaimer

1. The application/patent being disclaimed has been improperly identified since the name used to identify the application being disclaimed is incorrect. The correct name is Haghpassand, not Ron-Elazari-Volcani et al.

Response to Arguments

2. The rejections under 35 U.S.C. 101 have been overcome, based upon Applicant's addition of the term "non-transitory".

3. Applicant argued that Humes failed to disclose inbound lists which are "only one of which is active for a given request from a client." However, Humes performs this based on a "requested URL" – col. 6, line 18 and therefore it is "for a given request from a client." As restated below, it would have been obvious to one of ordinary skill in the art at the time of invention that if Humes had the ability to use an inbound allow list and an inbound deny list, that one or the other of the allow and deny lists could be independently used instead of using both lists, if the user wished to decrease security in a user system. Therefore, the result of using one list would have been independent of using the other list, and performable in any order.

4. Applicant argues that Cirasole failed to disclose "the unfriendly outbound list, the friendly inbound list, the unfriendly inbound list, being uniquely configured for each user account." Cirasole does teach the ability to uniquely configure a list in col. 5, lines 35-50 and col. 6, lines 1-5. It would have been obvious to one of ordinary skill in the art at

the time of invention that the ability to uniquely configure one list could be applied to all access lists used in Humes in order to enhance personal internet security.

5. Applicant argues that Humes fails to check the content of the requested document. In col. 5, lines 3-4, the requested web page URL, header, and body are filtered. Filtering the content is further taught in col. 5, lines 20-31, dealing with "objectionable material on the webpage.

6. Applicant argues that Gennaro fails to teach encrypting a portion of an email message selected by a user. The portion of a message selected by the user is the entire message. Applicant did not limit a portion to be less than the entire message.

7. Applicant argues that Gatz does not support client application authentication. Applicant did not claim this. Applicant's claim language is using "a configuration of the user's account to check the identity of at least one of (i) the requesting client and (ii) the requested resource. Applicant does not claim checking the application identity.

8. Applicant argued that Gatz failed to disclose having emails inaccessible to a user or deleting them. This is the concept of email blocking as taught in Gatz. When an email is blocked, it is rendered inaccessible to a user or deleted.

9. Applicant argued that Cirasole was not consistent with the limitations of claims 42-44. Applicant states that claims 42-44 require HTTP packets, but claims 42-44 never mention the use of HTTP packets. Applicant argues the number of lists in Cirasole as opposed to the claim limitations. It would have been obvious to one of ordinary skill in the art at the time of invention to use as many access filter lists as one

desired in Cirasole in order to improve the security of the system. An extra filter list is an extra layer of security.

10. Applicant argued in regard to claim 19 that Humes failed to include three paths: approving the request, terminating the request and terminating and re-routing the request. Applicant's claim language allows one of these options to fulfill the claim language – Applicant uses "either approving the request, terminating the request or terminating and re-routing the request."

11. Applicant argued that Humes failed to teach passing a request and alerting. The showing of a page indicating access is forbidden requires requesting the forbidden page (passing a request) and displaying the page (alerting).

12. Applicant argued in regard to claim 21 that Humes does not teach the limitations of the claim. As best understood, the Humes Forbidden page meets the limitations of rerouting requests to a replacement location.

Claim Rejections - 35 USC § 112

13. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

14. Claims 1, 2, 10, 12, 13, 14, 19, 21, 24, 27, 29, 32, 33, 38, 39, 40, 41, 42, 43, 44, 45, 46, 48, 50, 53, 54, and 57 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

15. For example, in claim 1, the paragraph (b) domain filtering engine is entirely unclear to understand. What element is "capable of using a friendly inbound list and an

unfriendly inbound list"? What element is "capable of both using a friendly outbound list and an unfriendly outbound list"? What element is "using a friendly inbound list and an unfriendly inbound list"?

16. Additionally issues exist with "one outbound list is independent of an outcome of use of the other outbound list or capable of using a friendly inbound list and an unfriendly inbound list". Is the domain engine capable of using both lists? Is the one outbound list capable of using both inbound lists? There are potentially two readings of the claim here, and the language must be clarified.

17. Applicant's claim language and lack of punctuation has entirely confused what Applicant's intended invention is, or what elements perform the steps in this section of the claim. It is entirely unclear what options are available to which elements of the claim.

18. Similar problems exist with claims 13, 14, 21, 24, 27, 29, 32, 42, 43, 44, 45, 46, 47, 50, and 57. Applicant's attempt to add as many options as possible to the claims, by adding options within options and not adding the appropriate punctuation, has confused the claims to the point where it is impossible to tell what options are present within what options in the claim. Consequently, the claims appear to have missing elements or method steps based on this obfuscation of the claims. It is not possible for one of ordinary skill in the art to ascertain what elements are required by the claims and what elements are optional in the claims as currently filed.

19. Claims 10 and 57 are rejected for failing to define the term HTTP within the claim.

20. Claims 12, 40, and 41 state “wherein for e-mail filtering", which is an incomplete clause. If this is referring to e-mail filtering in claim 1, there is insufficient antecedent basis within claim 1.

21. Claim 27 refers to “the privilege to create additional accounts.” There is insufficient antecedent basis for this within claim 1.

22. Claim 32 is rejected for failing to define the term URL within the claim.

23. Claim 45 states “…soft content exception list, and hard content exception list are being uniquely configured for each user account.” This is an incomplete phrase within the claim, and is therefore indefinite.

24. Claim 48 refers to an email exception list and an e-mail exception list. There is insufficient antecedent basis for “e-mail exception list”, but “email exception list is inconsistent with the use of “e-mail” throughout the claim set. There may be other instances of the “email” and “e-mail” irregularity that the Examiner has not identified.

25. Claim 57 refers to zero or more intermediary proxy servers. The claim is indefinite because it is not clear if Applicant intends to claim an intermediate proxy server or not from this claim language.

26. Claims 1, 2, 10, 12, 13, 14, 19, 32, 33, 38, 39, 42, 43, 44, 53, 54, and 57 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite in that it fails to point out what is included or excluded by the claim language. This claim is an omnibus type claim.

27. The claims in their entirety are replete with grammatical errors, incomplete phrases, and failure to use proper punctuation to clarify the claims. Applicant’s use of

multiple options within options, and the consistent use of the term “and/or” multiple times within the claims, has rendered the claims indefinite as to what elements are mandatory and what elements are optional within the claims. The Office has attempted to identify as many errors as possible within the claim set during this round of prosecution, but may have omitted some due to the number of claims and the amount of indefiniteness identified. Applicant is strongly urged to review the claims on their own in their entirety, identify the types of errors pointed out by the Examiner, and attempt to correct any that may not have been identified in an effort to advance prosecution.

Claim Rejections - 35 USC § 103

28. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

29. Claims 1-3, 10-14, 17-21, 23, 25, 27, 29-36, 38-43, 45-51, 53, and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gatz et al (US 2002/0049806) in view of Humes (US 5,996,011) in view of Cirasole et al. (US 5,987,606).

30. In regard to claim 1, Gatz disclosed a security and filtering software embodied in a non-transitory computer-readable medium, the software comprising:

(a) an administrative module that a user interacts with for creating user accounts and configuring those user accounts, Gatz, Figure 10 is administrative module, [0067]

the administrative module for accepting user inputs for configuration settings for inbound communications, for outbound communications or for inbound and outbound communications, (user inputs are input data, Gatz [0051], configuration settings for inbound communications or outbound communications are [0075], where settings can be overridden by a parent. Additional customized filtering taught in [0076]

Gatz failed to disclose:

(b) a domain filtering engine either capable of using a friendly outbound list and an unfriendly outbound list only one of which is active at any given time and such that use of one outbound list is independent of an outcome of use of the other outbound list or capable of using a friendly inbound list and an unfriendly inbound list in any order and such that use of one inbound list is independent of an outcome of use of the other inbound list, only one inbound list being active at any given time or capable of both using a friendly outbound list and an unfriendly outbound list only one of which is active at any given time and such that use of one outbound list is independent of the outcome of use of the other outbound list and using a friendly inbound list and an unfriendly inbound list in any order and such that use of one inbound list is independent of the outcome of the use of the other inbound list, only one inbound list being active at any given time the friendly outbound list, the unfriendly outbound list, the friendly inbound list, the unfriendly inbound list, being uniquely configured for each user account,

the using of the friendly or unfriendly outbound lists by the domain filtering engine involving checking user requested web resources against the friendly or unfriendly outbound lists, the using of the friendly or unfriendly inbound lists by the domain filtering

engine involving checking the identity of a requesting client against the friendly or unfriendly inbound lists.

However, Humes disclosed checking incoming web resources against either a friendly inbound list, an unfriendly inbound list, or both. (Humes, column 6, lines 18-38, friendly inbound list is Local-Allow list, unfriendly inbound list is Deny List. Only one of the lists is active at any given time because first the Local-Allow list is checked, and only subsequently is the Deny List checked)

Gatz was designed to prevent children from accessing inappropriate content on the Internet. Humes was designed to filter out inappropriate content on the Internet, while giving a user a chance to override some filter elements to permit content the particular user finds appropriate. It would have been obvious to one of ordinary skill in the art at the time of invention to incorporate Humes' filter into Gatz' system of protecting children from Inappropriate Internet content, in order to allow a user to access content that they might find appropriate but may have been filtered automatically by an automated filter (e.g. sites dealing with breast cancer) It would have been obvious to one of ordinary skill in the art at the time of invention that if Humes had the ability to use an inbound allow list and an inbound deny list, that one or the other of the allow and deny lists could be independently used instead of using both lists, if the user wished to decrease security in a user system.

Gatz and Humes failed to disclose the friendly outbound list, the unfriendly outbound list, the friendly inbound list, the unfriendly inbound list, being uniquely configured for each user account,

the using of the friendly or unfriendly inbound lists by the domain filtering engine involving checking the identity of a requesting client against the friendly or unfriendly inbound lists.

However, Cirasole disclosed:

the friendly outbound list, the unfriendly outbound list, the friendly inbound list, the unfriendly inbound list, being uniquely configured for each user account, (Cirasole col. 5, lines 35-50 and col. 6, lines 1-5, friendly inbound list is personal inclusive list, unfriendly inbound list is personal exclusive list)

the using of the friendly or unfriendly inbound lists by the domain filtering engine involving checking the identity of a requesting client against the friendly or unfriendly inbound lists. (col. 5, lines 51-57)

Gatz was designed to customize what a user could receive in terms of Internet content based on use of a family account with different levels for parents and children. Cirasole provided a personalized filter to customize content for a family account (col. 5, line 33). It would have been obvious to one of ordinary skill in the art at the time of invention to incorporate personalized filtering for family accounts into the family accounts of Gatz in order to allow the parent to see different content than the child based on the parent's personal selections.

31. In regard to claim 2, Humes further disclosed the software of claim 1, wherein the domain filtering engine also has an optional alert system for hard filtering, for soft filtering or for both hard and soft filtering. (alert for filtering is access FORBIDDEN page, Humes col. 5, lines 10-19)

32. In regard to claim 3, Gatz further disclosed the software of claim 1, wherein the domain filtering engine has an outbound privacy shield for blocking disapproved character strings representing confidential information without blocking character strings that do not represent confidential information. (outbound privacy shield is limiting public information available from child, [0074])

33. In regard to claim 10, Humes further disclosed the software of claim 1, wherein the domain filtering further includes an application server acting (i) internally, (ii) externally or (iii) internally and externally to communicate with the domain filtering engine and acting externally as a proxy server that receives requests from HTTP clients, forwards the requests to servers, receives a server response and forwards the server response to the HTTP clients. (Humes, proxy/cache server 110, col. 4, lines 45-60)

34. In regard to claim 11, Cirasole disclosed the software of claim 1, wherein the administrative module is also capable of configuring an automated configuration script file for accessing the global telecommunications network. (Cirasole, col. 4, lines 35-50, configuration is identifying filtering scheme and filtering elements)

35. In regard to claim 12, Gatz disclosed the software of claim 1, wherein for e-mail filtering includes at least one of (i) an option of hard e-mail filtering in which an incoming e-mail is deleted from a user e-mail inbox and (ii) includes an option for soft filtering in which an incoming e-mail remains in the user e-mail inbox but is inaccessible to the user. (Gatz, [0073])

36. In regard to claim 13, Humes and Cirasole disclosed the software of claim 1, further including a content filtering engine capable of performing content filtering including checking a content of a requested document against a friendly content inbound list, an unfriendly content inbound list, only one of the friendly content inbound list and the unfriendly content inbound list being active at any given time, the checking of one content inbound list independent of an outcome of a checking of the other inbound content list, the friendly content inbound list and the unfriendly content inbound list being uniquely configured for each user account, and if the content filtering involves hard filtering then against the unfriendly content inbound list either passing the requested document if the said content of the requested document is not on the unfriendly content inbound list or rejecting the requested document if the said content of the requested document is on the unfriendly content inbound list and for hard filtering against the friendly content inbound list either passing the requested document if the said content of the requested document is on the friendly content inbound list or rejecting the requested document if the said content of the requested document is not on the friendly content inbound list and if the content involves soft filtering then against the unfriendly content inbound list either approving the content of the requested document and passing the requested document if the said content is not on the unfriendly content inbound list or rejecting the content of the requested document and passing a remainder of the requested document if the said content is on the unfriendly content inbound list and against the friendly content inbound list either rejecting the requested document if parts of the content is not on the friendly content inbound list or

passing the requested document if the said content is on the friendly content inbound list. (Humes, column 6, lines 18-38, friendly inbound list is Local-Allow list, unfriendly inbound list is Deny List. Only one of the lists is active at any given time because first the Local-Allow list is checked, and only subsequently is the Deny List checked. Unique configuration of lists is taught in Cirasole as described in rejection for claim 1. Content filter in Humes, col. 5, lines 20-60)

37. In regard to claim 14, Gatz disclosed a security and filtering software embodied in a non-transitory computer-readable medium, the software, comprising:

(a) an administrative module that a user interacts with for creating user accounts and configuring those user accounts, (Gatz, Figure 10 is administrative module, [0067])

the administrative module for accepting user inputs for configuration settings for inbound communications, outbound communications or inbound and outbound communications (user inputs are input data, Gatz [0051], configuration settings for inbound communications or outbound communications are [0075], where settings can be overridden by a parent. Additional customized filtering taught in [0076])

Gatz failed to disclose

(b) a content filtering engine capable of performing content filtering including checking a content of a requested document against a friendly content inbound list and an unfriendly content inbound list in any order, a checking of the content of one of the content inbound lists independent of an outcome of a checking of the content of the other content inbound list, only one of the friendly content inbound list and the unfriendly content inbound list being active for a given request by a client, the friendly content

inbound list and the unfriendly content inbound list being uniquely configured for each user account, and if the content filtering involves hard filtering then against the unfriendly content inbound list either passing the requested document if the said content of the requested document is not on the unfriendly content inbound list or rejecting the requested document if the said content of the requested document is on the unfriendly content inbound list and against the friendly content inbound list either passing the requested document if the said content of the requested document is on the friendly content inbound list or rejecting the requested document if the said content of the requested document is not on the friendly content inbound list and if the content filtering involves soft filtering then against the unfriendly content inbound list either approving the content of the requested document and passing the requested document if the said content is not on the unfriendly content inbound list or rejecting the content of the requested document and passing a remainder of the requested document if the said content is on the unfriendly content inbound list and against the friendly content inbound list either rejecting the requested document if the said content is not on the friendly content inbound list or passing the requested document if the said content is on the friendly content inbound list.

However, Humes disclosed checking incoming web resources against either a friendly inbound list, an unfriendly inbound list, or both. (Humes, column 6, lines 18-38, friendly inbound list is Local-Allow list, unfriendly inbound list is Deny List. Only one of the lists is active at any given time because first the Local-Allow list is checked, and only subsequently is the Deny List checked) It would have been obvious to one of ordinary

skill in the art at the time of invention that if Humes had the ability to use an inbound allow list and an inbound deny list, that one or the other of the allow and deny lists could be independently used instead of using both lists, if the user wished to decrease security in a user system.

Gatz and Humes failed to disclose

the friendly content inbound list and the unfriendly content inbound list being uniquely configured for each user account

However, Cirasole disclosed

the friendly outbound list, the unfriendly outbound list, the friendly inbound list, the unfriendly inbound list, being uniquely configured for each user account, (Cirasole col. 5, lines 35-50 and col. 6, lines 1-5, friendly inbound list is personal inclusive list, unfriendly inbound list is personal exclusive list)

Gatz was designed to customize what a user could receive in terms of Internet content based on use of a family account with different levels for parents and children. Cirasole provided a personalized filter to customize content for a family account (col. 5, line 33). It would have been obvious to one of ordinary skill in the art at the time of invention to incorporate personalized filtering for family accounts into the family accounts of Gatz in order to allow the parent to see different content than the child based on the parent's personal selections

38. In regard to claim 17, Gatz disclosed the software of claim 14, wherein the content filtering engine has an inbound privacy shield for blocking scripting language functions for particular user accounts. Gatz, [0073]

39. In regard to claim 18, Humes disclosed the software of claim 13, wherein the content filtering engine, when performing at least one of soft filtering and hard filtering, can also replace a requested document that has been rejected with a replacement document selected by a user of the administrator account. (replacement document is FORBIDDEN page, Humes col. 5, lines 10-19)

40. In regard to claim 19, Humes disclosed the software of claim 1, wherein the domain filtering also includes with respect to both inbound and outbound requests for hard filtering either approving the request, terminating the request or terminating and re-routing the request. (Humes, column 6, lines 18-38)

41. In regard to claim 20, Humes disclosed the software of claim 1, wherein the domain filtering also includes with respect to both inbound and outbound requests for soft filtering passing disapproved requests and sending an alert to authorized recipients regarding the disapproved request. (alert is FORBIDDEN page, Humes col. 5, lines 10-19)

42. In regard to claim 21, Humes disclosed the software of claim 19, wherein the domain filtering also provides that, for requests that are terminated and re-rerouted, inbound communications are arranged so that an actual location of a highly sensitive resource is located in an unpublished location that is a replacement location to which requests rejected by the software are rerouted, wherein clients of approved users are

listed in the application server in the unfriendly inbound list and are sent by the application server to the replacement location, and wherein clients of unapproved users are not listed in the unfriendly inbound list and have their request sent to a published address that contains harmless information. (FORBIDDEN page, Humes col. 5, lines 10-19)

43. In regard to claim 23, Gatz and Cirasole disclosed the software of claim 1, wherein the domain filtering engine is capable of using from the administrative module a domain outbound exception list of web resources, is capable of using from the administrative module a domain inbound exception list of web resources and is capable of using from the administrative module a domain outbound exception list of web resources and a domain inbound exception list of web resources, the domain outbound exception list and the domain inbound exception list being uniquely configured for each user account. (Cirasole, col. 5, line 51 – col 6, line 13, domain inbound exception list is master-inclusive list, Gatz, [0081], domain outbound exception list is child's authorized buddy list) It would have been obvious to one of ordinary skill in the art that the lists of Gatz could be adapted to filter web resources, since Cirasole's lists were allow/deny lists as well.

44. In regard to claim 25, Cirasole disclosed the software of claim 1, said administrative module having list maintenance functions including list editing, list deleting, searching of lists, saving of lists, adding and deleting users, and having list maintenance functions including list editing, interchanging lists and importing and exporting lists. (Cirasole, col. 5, lines 31-50)

45. In regard to claim 27, Gatz disclosed the software of claim 1, said administrative module able to configure a range of access levels and being capable of creating three types of user accounts that have unique authentication credentials for each user account including an administrator account that is self-configuring and that controls automated services and selects for each account hard filtering or soft filtering, regular accounts with administrative privileges other than the privilege to create additional accounts, view information on any other accounts or configure automated services and regular accounts without administrative privileges. (Gatz, [0067])

46. In regard to claim 29, Gatz disclosed the software of claim 1, wherein the administrative module is capable of creating, modifying or reading the configuration settings or is capable of storing the configurations settings in memory, cache, encrypted files, plain text files, storage devices, computer storage media or as web resources. (Gatz, [0067], storage of configuration settings is inherent to operation of Gatz)

47. In regard to claim 30, Gatz disclosed the software of claim 27, wherein the administrative module is capable of at least one of (i) configuring the range of access levels for the user accounts created and (ii) configuring automated services. (Gatz, [0075])

48. In regard to claim 31, Gatz disclosed the software of claim 1, wherein the administrative module is capable of configuring at least one of (j) automated services and (ii) account configurations. (Gatz, [0075])

49. In regard to claim 32, Gatz disclosed the software of claim 23, wherein the domain filtering engine is capable of performing domain filtering, said domain filtering

including

checking the identity of a requesting client against the friendly inbound or unfriendly inbound list and domain inbound exception list and including for outbound web-based resource requests either

(i) checking user requested applications or

(ii) checking user requested domains or

(iii) checking user requested URLs or

(iv) checking user requested addresses or

(v) checking user requested links

against the friendly outbound list and/or the unfriendly outbound list and outbound exception list and then with respect to both inbound and outbound client communication requests for hard filtering unless overruled by the outbound exception list or domain inbound exception, list either approving the request, terminating the request or terminating and re-routing the request. (Gatz, Figure 6, items 84 and 85)

50. In regard to claim 33, Humes disclosed the software of claim 23, the soft domain filtering engine capable of performing domain filtering and for soft domain filtering unless overruled by the outbound exception list or domain inbound exception list passing disapproved requests and sending an alert to authorized recipients regarding the disapproved request. (Humes, column 6, lines 18-38, friendly inbound list is Local-Allow list, unfriendly inbound list is Deny List. Only one of the lists is active at any given time because first the Local-Allow list is checked, and only subsequently is the Deny List checked, alert is FORBIDDEN page)

51. In regard to claim 34, Humes disclosed the software of claim 33, wherein the soft domain filtering engine, for soft filtering, passes disapproved requests and sends alerts to authorized recipients regarding the disapproved requests. (Humes, column 6, lines 18-38)

52. In regard to claim 35, Gatz disclosed the software of claim 27, wherein the software is programmed to check an identity of a user who logs in and who presents a unique authentication credential prior to checking an identity of at least one of (i) a requesting client and.(ii) a requested resource. (Gatz, Figure 6, items 84 and 85)

53. In regard to claim 36, Gatz disclosed the software of claim 35, wherein the software is also programmed, upon a successful authentication of the user's credential, to use a configuration of the user's account to check the identity of at least one of (i) the requesting client and (ii) the requested resource. (Gatz, [0061])

54. In regard to claim 38, Gatz/Humes/Cirasole disclosed the software of claim 1, wherein the computer- readable medium is in a computer. See rejection for claim 1.

55. In regard to claim 39, Gatz/Humes/Cirasole disclosed the software of claim 1, wherein the computer- readable medium is in hardware. See rejection for claim 1.

56. In regard to claim 40, Gatz disclosed the software of claim 13, wherein for e-mail filtering includes an option of hard e-mail filtering in which an incoming e-mail is deleted from a user e-mail inbox. Gatz [0073]

57. In regard to claim 41, Gatz disclosed the software of claim 13, wherein for e-mail filtering includes an option of soft filtering in which an incoming e-mail remains in the user e-mail inbox but is inaccessible to the user. Gatz [0073]

58. In regard to claim 42, Cirasole disclosed the software of claim 13, wherein the content filtering engine is capable of using from the administrative module an unfriendly hard content exception list and/or a friendly hard content exception list, and/or an unfriendly soft content exception list and/or a friendly soft content exception list, the unfriendly soft content exception list and a friendly soft content exception list and unfriendly hard content exception list and the friendly hard content exception list, being uniquely configured for each user account. (Cirasole, col. 5, line 44 – col. 6, line 13)

59. In regard to claim 43, Cirasole disclosed the software of claim 42, wherein the content filtering engine is capable for hard filtering against a friendly hard content inbound list, an unfriendly hard content inbound list, a friendly hard content exception list and an unfriendly hard content exception list, the friendly content inbound list, the unfriendly content inbound list, only one of the friendly content inbound list mad the unfriendly content inbound list being active at any given time, and then for hard filtering against the unfriendly content inbound list either passing the requested document if the said content of the requested document is not on the unfriendly content inbound list or unless

overruled by the unfriendly hard content exception list rejecting the requested document if the said content of the requested document is on the unfriendly content inbound list and for hard filtering against the friendly content inbound list either unless overruled by the friendly hard content exception list passing the requested document if the said. content of the requested document is on the friendly content inbound list or rejecting the

requested document if the said content of the requested document is not on the friendly content inbound list. (Cirasole, col. 5, line 44 – col. 6, line 13)

60. In regard to claim 42, Cirasole disclosed the software of claim 42, wherein the content filtering engine is capable for soft filtering against the unfriendly content inbound list either unless overruled by the unfriendly soft content exception list approving the content of the requested document and passing the requested document if the said content is not on the unfriendly content inbound list or unless overruled by the unfriendly soft content exception list rejecting the content of the requested document and passing a remainder of the requested document if the said content is on the unfriendly content inbound list and/or for soft filtering against the friendly content inbound list either unless overruled by the friendly soft content exception list rejecting the requested document if the said content is not on the friendly content inbound list or unless overruled by the friendly soft content exception list passing the requested document if the said content is on the friendly content inbound list. (Cirasole, col. 5, line 44 – col. 6, line 13)

61. In regard to claim 45, Cirasole disclosed the software of claim 13, wherein a content filtering engine capable of using from the administrative module a soft content exception list, and using a hard content exception list, soft content exception list, and hard content exception list are being uniquely configured for each user account. (Cirasole, col. 5, line 44 – col. 6, line 13)

62. In regard to claim 46, Humes disclosed the software of claim 14, wherein the content filtering engine, when performing at least one of (i) hard filtering and (ii) soft filtering, is also able to replace a requested document that has been rejected with a

replacement document selected by a user of the administrator account. (Replacement document is FORBIDDEN page, Humes col. 5, lines 10-19)

63. In regard to claim 47, Gatz disclosed the software of claim 14, said content filtering also including e-mail filtering that checks a subject, a sender's address and a sender's domain against an unfriendly e-mail list, and friendly e-mail list. (Gatz, [0073])

64. In regard to claim 48, Gatz disclosed the software of claim 14, wherein the content filtering engine is capable of using from the administrative module an email exception list, the e-mail exception list being uniquely configured for each user account. (Gatz, [0073])

65. In regard to claim 49, Gatz disclosed the software of claim 48, said content filtering also including e-mail filtering that checks a subject, a sender's address and a sender's domain against an unfriendly e-mail list, a friendly e-mail list and an e-mail exception list. (Gatz, [0073])

66. In regard to claim 50, Gatz disclosed the software of claim 14, wherein the software is programmed to check an identity of a user who logs in and who presents a unique authentication credential prior to checking an identity of at least one of (i) a requesting client and (ii) a requested resource. (Gatz, Figure 6, items 84 and 85)

67. In regard to claim 51, Gatz disclosed the software of claim 50, wherein the software is also programmed, upon a successful authentication of the user's credential, to use a configuration of the user's account to check the identity of at least one of (i) the requesting client and (ii) the requested resource. (Gatz, [0061])

68. In regard to claim 53, Gatz/Humes/Cirasole disclosed the software of claim 14, wherein the computer-readable medium is in a computer. See rejection of Claim 14

69. In regard to claim 54, Gatz/Humes/Cirasole disclosed the software of claim 14, wherein the computer-readable medium is in hardware. See rejection of claim 14.

70. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gatz in view of Humes in view of Cirasole as applied to claim 1 above, and further in view of Schneier et al. (US 7,895,641).

In regard to claim 24, Gatz in view of Humes in view of Cirasole disclosed the software of claim 1. Gatz in view of Humes in view of Cirasole failed to disclose wherein the domain filtering, for soft filtering involves passing disapproved requests and sending an e-mail alert to authorized recipients regarding the disapproved request.

However, Schneier disclosed the use of email alerts for suspicious or security events. Schneier, col. 11, lines 16-33.

Gatz in view of Humes in view of Cirasole disclosed domain filtering of URLs that were inappropriate. Schneier disclosed sending email alerts for security events. The accessing of an inappropriate email is considered a type of security event. It would have been obvious to one of ordinary skill in the art at the time of invention to pass inappropriate URL access alerts on to the parent/administrator via an email alert for fast response.

71. Claims 26, 28, 37, and 52 and 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gatz in view of Humes in view of Cirasole as applied to claim 25 above, and further in view of Kocherlakota (US 6,785,705).

In regard to claim 26, Gatz in view of Humes in view of Cirasole disclosed the software of claim 25. Gatz disclosed in [0007] the common use of proxy servers, but failed to disclose administrative module having proxy chaining functions including proxy chaining routing. However, Kocherlakota disclosed establishing routing sessions through chaining proxy servers together over a network. Kocherlakota, col. 3, lines 10-20. It would have been obvious to one of ordinary skill in the art at the time of invention to incorporate proxy chaining into Gatz in order to allow for stronger security in making network connections.

In regard to claim 28, Gatz in view of Humes in view of Cirasole disclosed the software of claim 1, but failed to disclose said administrative module able to create a fourth type of user account namely one anonymous guest user account to be used by general users who have no authentication credentials. However, Kocherlakota disclosed using an anonymity proxy server to log into a network. Kocherlakota, col. 2, lines 61-64. It would have been obvious to one of ordinary skill in the art at the time of invention to allow for anonymous web access to Gatz in order to overcome security features unwanted by the user at the time of operation, as well as to protect the user's personal information when web surfing.

In regard to claim 37, Gatz in view of Humes in view of Cirasole disclosed the software of claim 35, but failed to disclose the software is also programmed that if the

software fails to authenticate the user, the first proxy server offers that user an opportunity to log in as an anonymous guest user. However, Kocherlakota disclosed using an anonymity proxy server to log into a network. Kocherlakota, col. 2, lines 61-64. It would have been obvious to one of ordinary skill in the art at the time of invention to allow for anonymous web access to Gatz in order to overcome security features unwanted by the user at the time of operation, as well as to protect the user's personal information when web surfing.

In regard to claim 52, Gatz in view of Humes in view of Cirasole disclosed the software of claim 50, but failed to disclose the software is also programmed that if the software fails to authenticate the user, the first proxy server offers that user an opportunity to log in as an anonymous guest user. However, Kocherlakota disclosed using an anonymity proxy server to log into a network. Kocherlakota, col. 2, lines 61-64. It would have been obvious to one of ordinary skill in the art at the time of invention to allow for anonymous web access to Gatz in order to overcome security features unwanted by the user at the time of operation, as well as to protect the user's personal information when web surfing.

72. In regard to claim 57, Gatz disclosed a security and filtering software embodied in a non-transitory computer-readable medium, the software comprising:

an administrative module that a user interacts with for creating user accounts and configuring those user accounts, (Gatz, Figure 10 is administrative module, [0067])

the administrative module for accepting user inputs for configuration settings for inbound communications, for outbound communications or for inbound and outbound

communications, (user inputs are input data, Gatz [0051], configuration settings for inbound communications or outbound communications are [0075], where settings can be overridden by a parent. Additional customized filtering taught in [0076])

Gatz failed to disclose

(b) a domain filtering engine either capable of using a friendly outbound list and an unfriendly outbound list only one of which is active at any given time and such that use of one outbound list is independent of an outcome of use of the other outbound list or capable of using a friendly inbound list and an unfriendly inbound list in any order and such that use of one inbound list is independent of an outcome of use of the other inbound list, only one inbound list being active at any given time or capable of both using a friendly outbound list and an unfriendly outbound list only one of which is active at any given time and such that use of one outbound list is independent of the outcome of use of the other outbound list and using a friendly inbound list and an unfriendly inbound list in any order and such that use of one inbound list is independent of the outcome of use of the other inbound list, only one inbound list being active at any given time the friendly outbound list, the unfriendly outbound list, the friendly inbound list, the unfriendly inbound list, being uniquely configured for each user account,

the using of the friendly or unfriendly outbound lists by the domain filtering engine involving checking user requested web resources against the friendly or unfriendly outbound lists, the using of the friendly or unfriendly inbound lists by the domain filtering engine involving checking the identity of a requesting client against the friendly or unfriendly inbound lists

wherein the domain filtering further includes an application server acting (i) internally, (ii) externally or (iii) internally and externally to communicate with the domain filtering engine and wherein the application server acts externally within a deployment of a chain of proxy servers including at least a first proxy server that receives requests from HTTP clients and forwards the requests through a zero or more intermediary proxy servers to a last proxy server, said last proxy server forwarding the requests to servers, and wherein the last proxy server receives a server response and forwards the server response through the zero or more intermediary proxy servers back to the first proxy server, which first proxy server forwards the server response to HTTP clients. However, Humes disclosed checking incoming web resources against either a friendly inbound list, an unfriendly inbound list, or both. (Humes, column 6, lines 18-38, friendly inbound list is Local-Allow list, unfriendly inbound list is Deny List. Only one of the lists is active at any given time because first the Local-Allow list is checked, and only subsequently is the Deny List checked)

Gatz was designed to prevent children from accessing inappropriate content on the Internet. Humes was designed to filter out inappropriate content on the Internet, while giving a user a chance to override some filter elements to permit content the particular user finds appropriate. It would have been obvious to one of ordinary skill in the art at the time of invention to incorporate Humes' filter into Gatz' system of protecting children from Inappropriate Internet content, in order to allow a user to access content that they might find appropriate but may have been filtered automatically by an automated filter (e.g. sites dealing with breast cancer) It would have been

obvious to one of ordinary skill in the art at the time of invention that if Humes had the ability to use an inbound allow list and an inbound deny list, that one or the other of the allow and deny lists could be independently used instead of using both lists, if the user wished to decrease security in a user system.

Gatz and Humes failed to disclose the friendly outbound list, the unfriendly outbound list, the friendly inbound list, the unfriendly inbound list, being uniquely configured for each user account,

the using of the friendly or unfriendly inbound lists by the domain filtering engine involving checking the identity of a requesting client against the friendly or unfriendly inbound lists.

However, Cirasole disclosed:

the friendly outbound list, the unfriendly outbound list, the friendly inbound list, the unfriendly inbound list, being uniquely configured for each user account, (Cirasole col. 5, lines 35-50 and col. 6, lines 1-5, friendly inbound list is personal inclusive list, unfriendly inbound list is personal exclusive list)

the using of the friendly or unfriendly inbound lists by the domain filtering engine involving checking the identity of a requesting client against the friendly or unfriendly inbound lists. (col. 5, lines 51-57)

Gatz was designed to customize what a user could receive in terms of Internet content based on use of a family account with different levels for parents and children. Cirasole provided a personalized filter to customize content for a family account (col. 5, line 33). It would have been obvious to one of ordinary skill in the art at the time of

invention to incorporate personalized filtering for family accounts into the family accounts of Gatz in order to allow the parent to see different content than the child based on the parent's personal selections.

73. Gatz disclosed in [0007] the common use of proxy servers, but failed to disclose administrative module having proxy chaining functions including proxy chaining routing. However, Kocherlakota disclosed establishing routing sessions through chaining proxy servers together over a network. Kocherlakota, col. 3, lines 10-20. It would have been obvious to one of ordinary skill in the art at the time of invention to incorporate proxy chaining into Gatz in order to allow for stronger security in making network connections.

74. Claims 6 and 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gatz in view of Humes in view of Cirasole as applied to claim 1 above, and further in view of Hughes et al. (US 6,065,055).

In regard to claim 6, Gatz in view of Humes in view of Cirasole disclosed the software of claim 1. Gatz in view of Humes in view of Cirasole failed to disclose including an automated scheduler that controls a launching of the software automatically and decides which user account to activate and when to shut off an access to a world wide web.

However, Hughes disclosed an automated scheduler that controls a launching of the software automatically and decides which user account to activate and when to shut off an access to a world wide web. (automated scheduler is start date/time and end date/time, col. 9, lines 1-3).

Gatz disclosed blocking inappropriate web sites by use of filtering, and Hughes disclosed analyzing content to determine when a web site may contain inappropriate content and adds the web site to a filter. It would have been obvious to one of ordinary skill in the art at the time of invention to automatically analyze websites to determine if they should be filtered or not, in order to give an extra layer of internet website protection.

In regard to claim 55, Gatz in view of Humes in view of Cirasole disclosed the software of claim 1. Gatz in view of Humes in view of Cirasole failed to disclose including an automated list updater that updates the friendly inbound list, the unfriendly inbound list, the friendly outbound list and the unfriendly outbound lists for each user account from links on the web.

However, Hughes disclosed an automated list updater that updates the friendly inbound list, the unfriendly inbound list, the friendly outbound list and the unfriendly outbound lists for each user account from links on the web. (automated list updater is filter list, col. 11, lines 37-54).

Gatz disclosed blocking inappropriate web sites by use of filtering, and Hughes disclosed analyzing content to determine when a web site may contain inappropriate content and adds the web site to a filter. It would have been obvious to one of ordinary skill in the art at the time of invention to automatically analyze websites to determine if they should be filtered or not, in order to give an extra layer of internet website protection.

75. Claim 9 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gatz in view of Humes in view of Cirasole as applied to claim 1 above, and further in view of Gennaro et al. (US 5,907,618).

In regard to claim 9, Gatz in view of Humes in view of Cirasole disclosed the software of claim 1, wherein the administrative module includes an editor, the editor including an editing pane. Gatz in view of Humes in view of Cirasole failed to disclose said editor also including an encryption said encryption function capable of encrypting all and capable of encrypting only a portion of an e-mail message, the portion being selected by the user.

However, Gennaro disclosed an encryption function capable of encrypting all or only a portion of an e-mail message selected by the user. Gennaro, col. 9, lines 18-30. The entire message is a portion of the message selected by the user.

Gatz transmitted email, but failed to disclose the capability of encrypting email. Gennaro disclosed symmetric encryption of email. It would have been obvious to one of ordinary skill in the art at the time of invention to incorporate email encryption into Gatz to further protect the privacy information of the child or other family users.

76. In regard to claim 56, Gennaro further disclosed the encryption function generates one or more symmetric encryption keys, the one or more encryption keys being uniquely associated with a text presented by a user of the editing pane. Gennaro, col. 9, lines 18-30.

Double Patenting

77. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

78. Claim 1 rejected on the ground of nonstatutory double patenting over claim 1 of U. S. Patent No. 7,587,499 since the claims, if allowed, would improperly extend the "right to exclude" already granted in the patent.

The subject matter claimed in the instant application is fully disclosed in the patent and is covered by the patent since the patent and the application are claiming common subject matter, as follows: Claim 1 of the instant application recites an administrative module for creating and configuring user accounts, accepting user inputs for configuration settings, and a domain filtering engine using friendly and unfriendly inbound and outbound lists. Claim 1 of the '499 patent discloses the administrative module, and a proxy server which has the same elements as the domain filtering engine in the instant application. It would have been obvious to one of ordinary skill in the art to implement the proxy server in the '499 patent as a "domain filtering engine". In addition, claim 1 of the instant application is a broader recitation of claim 1 of the '499 patent.

Furthermore, there is no apparent reason why applicant was prevented from presenting claims corresponding to those of the instant application during prosecution of the application which matured into a patent. See *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968). See also MPEP § 804.

Conclusion

79. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Nemovicher US 2002/0007453

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey R. Swearingen whose telephone number is (571)272-3921. The examiner can normally be reached on M-F 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lynn Feild can be reached on 571-272-2092. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey R Swearingen
Primary Examiner
Art Unit 2445

/Jeffrey R Swearingen/
Primary Examiner, Art Unit 2445